INFORMATION AND CONTROL 34, 107–122 (1977)

Characterization of the Decomposable Groups and Group Functions

K. KJELDSEN

HQ Def Com Nor, Oslo Mil/Akershus, Oslo 1, Norway

Decomposition of group functions is of considerable importance for the cascade synthesis of multivalued functions. We study cascades satisfying the more restrictive criterion "strongly decomposable." This approach introduces in a natural way a set of subgroups $\{G_m\}$ of G with the property that every m variable function into G_m is decomposable over G. Further, G_m is the maximal subgroup of G with this property. The decomposable subgroups of G are the subgroups of $\bigcap_{m=1}^{\infty} G_m$.

1. INTRODUCTION

Let X be a finite set, G a finite group, and H a subgroup of G. A function $f: X^m \to G$ is called a group function (into G). The set of group functions in m variables into G is denoted by $K_m(G)$. The elements of $K_1(G)$ are called the cell functions in G.

DEFINITION 1. $f: X^m \to G$ is decomposable over G if there exist n, $\lambda: \{1, 2,..., n\} \to \{1, 2,..., m\}$, and cell functions f_i such that

$$f(x_1, x_2, ..., x_m) = \prod_{i=1}^{n} f_i(x_{\lambda(i)}).$$

H is decomposable over G iff all $f \in \bigcup_{m=1}^{\infty} K_m(H)$ are decomposable over G.

Clearly all cell functions are decomposable over G. For $m \geqslant 2$, $f \in K_m(G)$ is decomposable over G if and only if there exist n, $f_i \in K_{m-1}(G)$, $g_i \in K_1(G)$, $i = 1, 2,..., n$, such that

$$f(x_1, x_2, ..., x_m) = \prod_{i=1}^{n} f_i(x_1, x_2, ..., x_{m-1})\, g_i(x_m), \tag{1}$$

with each f_i decomposable over G.

The decomposable group functions are of considerable importance for the realization of the functions at the output of cellular cascades. In other papers studying decomposition of group functions, for example, Yoeli and Turner (1967), Elspas and Stone (1967), Kolp (1972, 1976), Eq. (1) has been used

ISSN 0019-9958

inductively to find decomposable subgroups. Sufficient conditions were put on H in order to ensure that for all $f \in K_m(H)$, (1) has a solution with $f_i \in K_{m-1}(H)$, $i = 1, 2, \ldots, n$. By induction applied to the f_i's (one less variable than f) a set of decomposable subgroups was found.

This supports the importance of studying subgroups satisfying the more restrictive definition of decomposable (which we call strongly decomposable) subgroups as defined below.

DEFINITION 2. $f \in K_m(H)$ is strongly decomposable over G if $m = 1$, or $m \geqslant 2$ and there exist n, $f_i \in K_{m-1}(H)$, $g_i \in K_1(G)$, $i = 1, 2, \ldots, n$, such that

$$f(x_1, x_2, \ldots, x_m) = \prod_{i=1}^{n} f_i(x_1, x_2, \ldots, x_{m-1})\, g_i(x_m),$$

with all the f_i's strongly decomposable over G.

H is strongly decomposable over G iff all $f \in \bigcup_{m=1}^{\infty} K_m(H)$ are strongly decomposable over G.

Clearly a strongly decomposable subgroup of G is decomposable. Kolp (1976) has shown that the decomposable subgroups of G constitute a lattice invariant under inner automorphisms of G. If $D(G)$ is the largest decomposable subgroup of G, then $D(G)$ is normal, and H is decomposable if and only if $H \subset D(G)$. It can be concluded from Kolp's paper that $D(G)$ is a subgroup of the commutator group $[G, G]$ of G.

In Section 2 we determine the set of strongly decomposable subgroups of G. This set contains a unique largest subgroup $S(G)$ of G. Accordingly, $D(G)$ is bounded by

$$S(G) \subset D(G) \subset [G, G]. \tag{2}$$

In Section 3 we make a closer study of the decomposition of functions in m variables, m fixed. A set of subgroups $\{G_m\}$ of G is defined such that all $f \in K_m(G_m)$ are decomposable over G.

In Section 5 we prove that G_m is the maximal subgroup of G with this property. Those subgroups satisfy

$$G_1 = G, \quad G_m \supset G_{m+1}, \qquad \text{and} \qquad \bigcap_{m=1}^{\infty} G_m = S(G).$$

In Section 4 we give canonical representations of the decomposable functions, which are utilized in Section 5 to characterize the decomposable subgroups of G.

In Section 6 we determine the decomposable subgroups for some of the classical groups.

The case when the number $|X|$ of elements in X equals 1 is trivial. So we assume throughout that $|X| \geqslant 2$.

2. Strongly Decomposable Groups

Let $f \in K_m(G)$. For each $x \in X^m$ we define $f_x \in K_m(G)$ by

$$\begin{aligned} f_x(y) &= f(x) \quad \text{if} \quad y = x, \\ &= e \quad \text{if} \quad y \neq x, \end{aligned} \tag{3}$$

where e denotes the identity element of G. Since $f = \prod_{x \in X^m} f_x$, and the product of (strongly) decomposable functions is (strongly) decomposable, f is (strongly) decomposable if every f_x is (strongly) decomposable. The converse is not true.

Let $h \in G$. Define $f^m_{h,x} \in K_m(G)$ by

$$\begin{aligned} f^m_{h,x}(y) &= h \quad \text{if} \quad y = x, \\ &= e \quad \text{if} \quad y \neq x. \end{aligned} \tag{4}$$

Lemma 1. *H is (strongly) decomposable over G if and only if for all m, all $x \in X^m$, all $h \in H$, $f^m_{h,x}$ is (strongly) decomposable.*

This trivial result has some important implications. First the (strongly) decomposable subgroups of G are independent of the set X if X contains more than one element.

Second the problem of finding (strongly) decomposable groups is reduced to test whether all $f^m_{h,x}$ are (strongly) decomposable or not. This is a sufficient simplification to determine all strongly decomposable subgroups of G.

Definition 3. Let G be a group and H a subgroup of G. Denote by H^* the group generated by $\{uhu^{-1}h^{-1} \mid u \in G, h \in H\}$.

The groups H^* are important for the theory of the strongly decomposable groups as shown in the theorem below. H^* is the mutual commutator of G and H (see Zassenhaus, 1956, p. 81).

Theorem 1. *H is strongly decomposable if and only if $H \subset H^*$.*

Proof. We prove by induction on m that all $f \in K_m(H)$ are strongly decomposable if $H \subset H^*$. All $f \in K_1(H)$ are strongly decomposable by definition. Suppose we have shown that all $f \in K_{m-1}(H)$, $m \geqslant 2$, are strongly decomposable. On this assumption we shall prove that all $f^m_{h,x} \in K_m(H)$ are strongly decomposable. By Lemma 1 and the induction hypothesis it then follows that H is strongly decomposable.

Let $h \in H$, $x = (x_1, x_2, \ldots, x_m) \in X^m$. There exist n, $h_i \in H$, $u_i \in G$, $i = 1, 2, \ldots, n$ such that

$$h = \prod_{i=1}^{n} u_i h_i u_i^{-1} h_i^{-1}.$$

Define $\phi_i \in K_{m-1}(H)$, $\psi_i \in K_1(G)$ by

$$\begin{aligned} \phi_i(y_1,\ldots,y_{m-1}) &= h_i \quad \text{if} \quad (y_1,\ldots,y_{m-1}) = (x_1,\ldots,x_{m-1}), \\ &= e \quad \text{otherwise}, \end{aligned} \tag{5}$$

$$\begin{aligned} \psi_i(y_m) &= u_i \quad \text{if} \quad y_m = x_m, \\ &= e \quad \text{otherwise}. \end{aligned} \tag{6}$$

Clearly $f^m_{h,x} = \prod_{i=1}^n \psi_i\phi_i\psi_i^{-1}\phi_i^{-1}$. Since by the induction hypothesis ϕ_i and ϕ_i^{-1} are strongly decomposable, so is $f^m_{h,x}$.

Conversely, suppose that H is strongly decomposable. We shall show that $H \subset H^*$. For all $h \in H$, all $x = (x_1, x_2) \in X^2$, the function $f^2_{h,x}$ is strongly decomposable. Accordingly, there exist n, $f_i \in K_1(G)$, $g_i \in K_1(H)$, $i = 1, 2,\ldots, n$, such that

$$f^2_{h,x}(y_1, y_2) = \prod_{i=1}^n f_i(y_2)\, g_i(y_1).$$

Fix $y \neq x_1$, $z \neq x_2$.

Put $\alpha_i = f_i(x_2)$, $\beta_i = f_i(z)$, $\gamma_i = g_i(x_1)$, $\delta_i = g_i(y)$. Then $\alpha_i, \beta_i \in G$, γ_i, $\delta_i \in H$ and

$$\begin{aligned} f(x_1, x_2) &= \prod_{i=1}^n \alpha_i\gamma_i = h, \\ f(y, x_2) &= \prod_{i=1}^n \alpha_i\delta_i = e, \\ f(x_1, z) &= \prod_{i=1}^n \beta_i\gamma_i = e, \\ f(y, z) &= \prod_{i=1}^n \beta_i\delta_i = e, \end{aligned} \tag{7}$$

Put $\alpha_i' = \alpha_i\delta_i$, $\beta_i' = \beta_i\delta_i$, $\gamma_i' = \delta_i^{-1}\gamma_i$. Then $\alpha_i', \beta_i' \in G$, $\gamma_i' \in H$, and (7) is equivalent to

$$\begin{aligned} \prod_{i=1}^n \alpha_i'\gamma_i' &= h, \\ \prod_{i=1}^n \alpha_i' &= e, \\ \prod_{i=1}^n \beta_i'\gamma_i' &= e, \\ \prod_{i=1}^n \beta_i' &= e. \end{aligned} \tag{8}$$

Put $a_i = \alpha_1'\alpha_2' \cdots \alpha_i'$, $b_i = \beta_1'\beta_2' \cdots \beta_i'$. It follows from the fisrt and third equation in (8) that

$$h = \left(\prod_{i=1}^{n} a_i\gamma_i' a_i^{-1}\right) a_n ,$$

$$e = \left(\prod_{i=1}^{n} b_i\gamma_i' b_i^{-1}\right) b_n .$$

By the second and fourth equation in (8) $a_n = b_n = e$. Accordingly,

$$\begin{aligned} h &= \prod_{i=1}^{n} a_i\gamma_i' a_i^{-1}, \\ e &= \prod_{i=1}^{n} b_i\gamma_i' b_i^{-1}. \end{aligned} \tag{9}$$

Define $c_i = \gamma_{i-1}'\gamma_{i-2}' \cdots \gamma_1' a_i$, $d_i = \gamma_{i-1}'\gamma_{i-2}' \cdots \gamma_1' b_i$. Then (9) is equivalent to

$$\begin{aligned} h &= \left(\prod_{i=1}^{n} c_i\gamma_i' c_i^{-1}\gamma_i'^{-1}\right)\gamma_n'\gamma_{n-1}' \cdots \gamma_1', \\ e &= \left(\prod_{i=1}^{n} d_i\gamma_i' d_i^{-1}\gamma_i'^{-1}\right)\gamma_n'\gamma_{n-1}' \cdots \gamma_1'. \end{aligned} \tag{10}$$

Accordingly, $h = (\prod_{i=1}^{n} c_i\gamma_i' c_i^{-1}\gamma_i'^{-1})(\prod_{i=1}^{n} d_i\gamma_i' d_i^{-1}\gamma_i'^{-1})^{-1}$ with $c_i, d_i \in G$, $\gamma_i' \in H$. Hence $h \in H^*$. Q.E.D.

The strongly decomposable subgroups of G possess many properties. Some are summarized in the corollaries below.

COROLLARY 1. *H^* is a normal subgroup of G.*

Proof. Let $g \in G$. It suffices to show that $gxg^{-1} \in H^*$ when x is a generator of H^*. Let therefore $u \in G$, $h \in H$ be arbitrary. Then

$$g(uhu^{-1}h^{-1})\,g^{-1} = [(gu)\,h(gu)^{-1}\,h^{-1}] \cdot [hgh^{-1}g^{-1}] \in H^*. \qquad \text{Q.E.D.}$$

COROLLARY 2. *H is strongly decomposable if and only if aHa^{-1} is strongly decomposable, $a \in G$.*

Proof. A generator of $(aHa^{-1})^*$ has the form $u(aha^{-1})\,u^{-1}(ah^{-1}a^{-1})$ with $u \in G$, $h \in H$. $u(aha^{-1})\,u^{-1}(ah^{-1}a^{-1}) = [(ua)\,h(ua)^{-1}\,h^{-1}] \cdot [hah^{-1}a^{-1}] \in H^*$. Accordingly, $(aHa^{-1})^* \subset H^*$. By the symmetry we conclude that $(aHa^{-1})^* = H^*$. Since H^* is normal, $H^* = (aHa^{-1})^*$ contains H if and only if it contains aHa^{-1}. Q.E.D.

COROLLARY 3. *If H and H' are strongly decomposable subgroups of G, then $[H \cup H']$, the group generated by H and H', is strongly decomposable.*

Proof. If $g \in [H \cup H']$, then $g = h_1 h_2 \cdots h_n$ with $h_i \in H$ or $h_i \in H'$. Since each $h_i \in H^*$ or H'^*, $g \in [H^* \cup H'^*] \subset [H \cup H']^*$. Q.E.D.

COROLLARY 4. *H is strongly decomposable if and only if H^* is equal to the group generated by H and the conjugates of H.*

Proof. By Corollaries 2 and 3, H is strongly decomposable if and only if $H^* \supset [\bigcup_{u \in G} uHu^{-1}]$. The generator $uhu^{-1}h^{-1}$, $u \in G$, $h \in H$, of H^* is an element of $[(uHu^{-1}) \cup H]$. Accordingly, $H^* \subset [\bigcup_{u \in G} uHu^{-1}]$. Q.E.D.

COROLLARY 5. *If H is a normal subgroup of G, then H is strongly decomposable if and only if $H = H^*$.*

If H is a normal subgroup of G, then $uhu^{-1} \in H$. Accordingly, $uhu^{-1}h^{-1} \in H$ in this case. Therefore H^* is always a subgroup of H when H is normal.

It follows from Corollary 3 (the upper lattice property) and Corollary 4 that

COROLLARY 6. *There exists a maximal strongly decomposable subgroup $S(G)$ of G. Further, $S(G)$ is a normal subgroup of G.*

We shall now determine the maximal strongly decomposable subgroup of G.

DEFINITION 4. A set of subgroups $\{G_r \mid r = 1, 2, \ldots\}$ is recursively defined by $G_1 = G$, and $G_r = G_{r-1}^*$ if $r > 1$.

It follows from Corollary 1 that G_r is a normal subgroup of G. Therefore $G_{r+1} = G_r{}^*$ is a subgroup of G_r. We have thus obtained a descending chain $G_1 \supset G_2 \supset \cdots \supset G_r \supset G_{r+1} \cdots$ of groups. Since G is finite, $G_{r_0} = G_{r_0+1}$ for some r_0. For all $i > r_0$, $G_i = G_{r_0}$.

THEOREM 2. $S(G) = \bigcap_{r=1}^{\infty} G_r$.

Proof. It is clear that $(\bigcap_{r=1}^{\infty} G_r)^* = \bigcap_{r=1}^{\infty} G_r = G_{r_0}$. Accordingly $\bigcap_{r=1}^{\infty} G_r$ is strongly decomposable and normal. By induction on r it is easily proved that every strongly decomposable subgroup of G is contaiend in G_r. Q.E.D.

3. INTERPRETATION OF G_m

DEFINITION 5. A subgroup H of G is m-decomposable if all $f \in K_m(H)$ are decomposable over G.

Clearly every subgroup of a m-decomposable group is m-decomposable, and there exists a maximal m-decomposable subgroup H_m of G. Further H_m is a

normal subgroup of G, and $H_m \supset H_{m+1}$. The maximal decomposable group $D(G)$ of G is equal to $\bigcap_{m=1}^{\infty} H_m$. In this section we shall show that the groups G_m introduced in the previous section are m-decomposable subgroups of G. In Section 5 it will be proved that G_m is the maximal m-decomposable subgroup of G. Hence $D(G) = S(G)$.

THEOREM 3. *G_m is m-decomposable over G.*

Proof. $G = G_1$ is 1-decomposable. Suppose we have shown that G_{m-1} is $(m-1)$-decomposable. If on this assumption we show that G_m is m-decomposable, it follows by induction that G_r is r-decomposable for all r. Clearly it suffices to show that all $f^m_{h,x} \in K_m\ (G_m)$ are decomposable. There exist n, $h_i \in G_{m-1}$, $u_i \in G$, $i = 1, 2, \ldots, n$, such that

$$h = \prod_{i=1}^{n} u_i h_i u_i^{-1} h_i^{-1}.$$

Let $\phi_i \in K_{m-1}(G_{m-1})$, $\psi_i \in K_1(G)$ be defined as in (5) and (6). Clearly $f^m_{h,x} = \prod_{i=1}^{n} \psi_i \phi_i \psi_i^{-1} \phi_i^{-1}$. Since by the induction hypothesis ϕ_i and ϕ_i^{-1} are decomposable, so is $f^m_{h,x}$. Q.E.D.

4. CANONICAL FORMS OF DECOMPOSABLE FUNCTIONS

We shall give canonical representations of the decomposable group functions. These canonical forms will be utilized in the next section to show that G_m is the maximal m-decomposable subgroup of G. However, in order to obtain the appropriate representations a result about the groups G_m will be needed. This is given in the lemma below.

LEMMA 2. *If $g \in G_p$, $h \in G_q$, then $ghg^{-1}h^{-1} \in G_{p+q}$.*

Proof. The proof is by induction on q. The lemma is true for all p if $q = 1$ by the definition of G_{p+1}. Suppose it has been proved for $q - 1$ and all p. We shall show that it is also valid for q and all p, and by induction for all p and q.

If $h = h_1 h_2$ with $h_1, h_2 \in G_q$, then $ghg^{-1}h^{-1} = (gh_1g^{-1}h_1^{-1})\, h_1(gh_2g^{-1}h_2^{-1})\, h_1^{-1}$. If $gh_2g^{-1}h_2^{-1} \in G_{p+q}$, then $h_1(gh_2g^{-1}h_2^{-1})\, h_1^{-1} \in G_{p+q}$ since G_{p+q} is a normal subgroup of G. It suffices therefore to show that $ghg^{-1}h^{-1} \in G_{p+q}$ when $h = a\beta a^{-1}\beta^{-1}$ with $a \in G_1$, $\beta \in G_{q-1}$, i.e., h is a generator of G_q.

Put

$$x = gag^{-1}a^{-1}, \quad y = ag\beta g^{-1}a^{-1}, \quad z = g\beta g^{-1}\beta^{-1}, \quad u = \beta a^{-1}\beta^{-1}.$$

Then

$$ghg^{-1}h^{-1} = (xyx^{-1}y^{-1})\, a(zuz^{-1}u^{-1})\, a^{-1}.$$

Now $x \in G_{p+1}$ since $g \in G_p$ and $a \in G_1$, and $y \in G_{q-1}$ since $\beta \in G_{q-1}$ and G_{q-1} is normal. By the induction hypothesis, $xyx^{-1}y^{-1} \in G_{p+q}$. Further $z \in G_{p+q-1}$ by the induction hypothesis since $g \in G_p$ and $\beta \in G_{q-1}$. Accordingly $zuz^{-1}u^{-1} \in G_{p+q}$. Since G_{p+q} is normal it also follows that $a(zuz^{-1}u^{-1})\, a^{-1} \in G_{p+q}$. Q.E.D.

If f is a decomposable function, then a representation of f of the type given in (11) below will be called a canonical form of f.

Put $I_{m,k} = \{(i_1, i_2, \ldots, i_k) \mid 1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant m\}$.

THEOREM 4. *$f \in K_m(G)$ is decomposable if and only if there exist $\phi_{i_1 \ldots i_k} \in K_k(G_k)$, $(i_1, \ldots, i_k) \in I_{m,k}$, $k = 1, 2, \ldots, m$, such that*

$$f(x_1, x_2, \ldots, x_m) = \prod_{k=1}^{m} \prod_{(i_1, \ldots, i_k) \in I_{m,k}} \phi_{i_1 \ldots i_k}(x_{i_1}, \ldots, x_{i_k}). \tag{11}$$

Proof. $\phi_{i_1 \ldots i_k} \in K_k(G_k)$ is decomposable by Theorem 3. The product of decomposable functions is decomposable. Accordingly, if there exist $\phi_{i_1 \ldots i_k} \in K_k(G_k)$, $(i_1, \ldots, i_k) \in I_{m,k}$, $k = 1, 2, \ldots, m$, satisfying (11), then f is decomposable.

The proof of the converse statement is tricky. To clarify this proof, we shall first illustrate the ideas through an easy example. Lemma 2 is used every time two functions are commuted.

Suppose that

$$f(x_1, x_2, x_3) = f_1(x_2) f_2(x_1) f_3(x_3) f_4(x_1)$$

is a decomposition of f. First we factor out the functions in x_1. Commuting f_3 and f_4 gives

$$f = f_1(x_2)\, g(x_1)\, f_3(x_3)\, \phi_1(x_1, x_3), \qquad \text{where} \qquad g = f_2 f_4 \text{ and } \phi_1 \in K_2(G_2).$$

Commuting f_1 and g gives

$$f = g(x_1) f_1(x_2)\, \phi_2(x_1, x_2) f_3(x_3)\, \phi_1(x_1, x_3),$$

with $\phi_2 \in K_2(G_2)$. Commuting ϕ_2 and f_3 gives

$$f = g(x_1) f_1(x_2) f_3(x_3)\, \phi_2(x_1, x_2)\, \psi(x_1, x_2, x_3)\, \phi_1(x_1, x_3),$$

with $\psi \in K_3(G_3)$. Finally by commuting ψ and ϕ_1 we get

$$f = g(x_1) f_1(x_2) f_3(x_3)\, \phi_2(x_1, x_2)\, \phi_1(x_1, x_3)\, \psi'(x_1, x_2, x_3),$$

where $\psi' \in K_3(G_5) \subset K_3(G_3)$, which is a representation of the canonical form (11).

Let $\nu\colon \{1, 2,..., 2^m - 1\} \to \bigcup_{k=1}^{m} I_{m,k}$ be any one to one mapping such that if $\nu(i) \in I_{m,k}$, $\nu(i') \in I_{m,k'}$ and $k < k'$, then $i < i'$. If $\nu(j) = (i_1, i_2, ..., i_k)$, then we define

$$x(\nu(j)) = (x_{i_1}, x_{i_2}, ..., x_{i_k}). \tag{12}$$

Suppose that f is decomposable. We shall show that

$$f(x_1, x_2, ..., x_m) = \prod_{j=1}^{2^m-1} \phi_j(x(\nu(j))) \tag{13}$$

for suitable functions ϕ_j, $j = 1, 2,..., 2^m - 1$, with $\phi_j \in K_k(G_k)$ if $\nu(j) \in I_{m,k}$. This will prove the theorem.

Since f is decomposable there exist n, $\lambda\colon \{1, 2,..., n\} \to \{1, 2,..., m\}$ and cell functions f_i such that

$$f(x_1, x_2, ..., x_m) = \prod_{i=1}^{n} f_i(x_{\lambda(i)}). \tag{14}$$

The first step in order to obtain a representation (13) for f is to remove all functions in $x(\nu(1))$ from the product in (14), and substitute these functions with one single function $\phi_1(x(\nu(1)))$. Similarly for the functions in $x(\nu(2))$ etc. This is done in the following way:

Suppose we have already factored out all functions in the variable $x(\nu(1))$, all functions in the variable $x(\nu(2))$,..., all functions in the variable $x(\nu(N))$. More specifically, we assume that

$$f(x_1, x_2, ..., x_m) = \prod_{j=1}^{N} \phi_j(x(\nu(j))) \prod_{k=1}^{N'} g_k(x(\nu(j_k))), \tag{15}$$

with $j_k > N$ for all k, $\phi_j \in K_s(G_s)$ if $\nu(j) \in I_{m,s}$, and $g_k \in K_q(G_q)$ if $\nu(j_k) \in I_{m,q}$.

The next step is to factor out a function $\phi_{N+1}(x(\nu(N + 1)))$. Thus we obtain a representation (15) of f with N replaced by $N + 1$. By induction on N we get a representation of f of the desired type (13).

If $N = 2^m - 1$, (15) is of the type (13) and we are through. Also if $N < 2^m - 1$ and $j_k \neq N + 1$ for all k, $k = 1, 2,..., N'$, we are through. Simply, put $\phi_{N+1}(x(\nu(N + 1))) = e$ in this case.

Otherwise let $J = \{k_1, k_2, ..., k_p\}$ be the set of values k such that $j_k = N + 1$ in the representation (15). Further assume that $k_p \geqslant k_r$ for all r. Put $\psi_{k_p} = g_{k_p}$ and define recursively for $2 \leqslant t \leqslant k_p$

$$\psi_{t-1} = \psi_t \qquad \text{if} \quad t - 1 \notin J$$

and

$$\psi_{t-1} = g_{t-1}\psi_t \qquad \text{if} \quad t - 1 \in J.$$

If $t - 1 \notin J$, define γ_{t-1} by

$$\psi_{t-1} g_{t-1} \gamma_{t-1} = g_{t-1}\psi_t. \tag{16}$$

Put $\phi_{N+1}(x(\nu(N+1))) = \psi_1$. Then (15) is equivalent to

$$f(x_1, x_2, \ldots, x_m) = \prod_{j=1}^{N+1} \phi_j(x(\nu(j))) \prod_{\substack{k<k_p \\ k\notin J}} g_k\gamma_k \prod_{s=k_p+1}^{N'} g_s . \tag{17}$$

If $\nu(N+1) = (i_1, i_2, \ldots, i_k)$, $t-1 \notin J$, $g_{t-1} = g_{t-1}(x_{j_1}, \ldots, x_{j_r})$, then

$$\gamma_{t-1} = \gamma_{t-1}(x_{i_1}, \ldots, x_{i_k}, x_{j_1}, \ldots, x_{j_r}) = \gamma_{t-1}(x_{p_1}, \ldots, x_{p_u}),$$

where $p_1 < p_2 < \cdots < p_u$ and $k < u \leqslant k+r$. By (16) and Lemma 2 $\gamma_{t-1} \in K_u(G_{k+r}) \subset K_u(G_u)$ since $\psi_{t-1} = \psi_t$ in this case. Also $\nu^{-1}((p_1, p_2, \ldots, p_u)) > N+1$. Accordingly (17) is of the type (15) with N replaced by $N+1$. Q.E.D.

A decomposable function need not be strongly decomposable. For instance, a function $f(x_1, x_2)$ in two variables is decomposable if and only if $f(x_1, x_2) = g(x_1)\, h(x_2)\, \phi(x_1, x_2)$ for suitable functions $g, h \in K_1(G)$ and a suitable $\phi \in K_2(G_2)$. Here $G_2 = [G, G]$ is the commutator subgroup of G. If G is a group such that $S(G) = G_2$, then $f(x_1, x_2)$ is strongly decomposable if and only if $f(x_1, x_2) = h(x_2)\, \phi(x_1, x_2)$ for suitable, $h \in K_1(G), \phi \in K_2(G_2)$. For several groups $S(G) = G_2$ and $G_2 \neq G$. For instance the symmetric groups have this property (see Section 6).

5. Classification of the Decomposable Groups

In Section 3 we showed that G_m is an m-decomposable subgroup of G. There also exists a unique maximal subgroup of G which is m-decomposable. In this section we shall show that G_m is the maximal m-decomposable subgroup of G. The canonical representation (11) of a decomposable function will be used in the proof. Also a simple property about G_m (given in the corollary to the lemma below) will be needed.

The center $Z(G)$ of G consists of those elements of G which commute with all elements in G.

Lemma 3. *If $p \leqslant q$, then $G_q/G_{p+q} \subset Z(G_p/G_{p+q})$.*

Proof. $G_p \supset G_q$ since $p \leqslant q$. If $g \in G_p$, $h \in G_q$, then $gh \equiv hg \bmod G_{p+q}$ by Lemma 2. Q.E.D.

Corollary. *If $p \leqslant q$, then G_q/G_{p+q} is abelian.*

Theorem 5. *G_m is the maximal m-decomposable subgroup of G.*

Proof. G_m is m-decomposable by Theorem 3. We show that G_m is the maximal subgroup of G with this property. Without loss of generality we may

assume that $X = \{0, 1\}$. Put $\mathbf{0} = (0, 0, \ldots, 0)$. It clearly suffices to show that $f^m_{u,\mathbf{0}} \in K_m(G_m)$ when decomposable.

Suppose we have shown that the representation (11) for $f^m_{u,\mathbf{0}}$ has been reduced to

$$f^m_{u,\mathbf{0}}(x_1, x_2, \ldots, x_m) = \prod_{k=N}^{m} \prod_{(i_1,\ldots,i_k)\in I_{m,k}} \phi_{i_1\cdots i_k}(x_{i_1}, \ldots, x_{i_k}), \tag{18}$$

with all $\phi_{i_1\cdots i_k} \in K_k(G_k)$. If $N = m$, then $f^m_{u,\mathbf{0}} = \phi_{1\cdots m} \in K_m(G_m)$, and we are through.

If $N < m$ we shall show that $f^m_{u,\mathbf{0}}$ also has a representation (18) with N replaced by $N + 1$. Continuing with this new expression for $f^m_{u,\mathbf{0}}$ etc., we finally get $f^m_{u,\mathbf{0}} \in K_m(G_m)$. The theorem therefore follows from Lemma 4 and Lemma 5 below. Q.E.D.

LEMMA 4. *Fix $N < m$. If $f^m_{u,\mathbf{0}}$ has a representation (18) with all $\phi_{i_1\cdots i_k} \in K_k(G_k)$, then $f^m_{u,\mathbf{0}} \in K_m(G_{N+1})$.*

Proof. We show that $u \in G_{N+1}$. Put $w(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} x_i$, i.e., the number of coordinates in $(x_1, x_2, \ldots, x_n)$ which are equal to 1. Since

$$u = \prod_{(x_1,\ldots,x_m)\in X^m} (f^m_{u\,\mathbf{0}}(x_1, \ldots, x_m))^{(-1)^{w(x_1,\ldots,x_m)}},$$

it follows that

$$u \equiv \prod_{(x_1,\ldots,x_m)\in X^m} \Big(\prod_{(i_1,\ldots,i_N)\in I_{m,N}} \phi_{i_1\cdots i_N}(x_{i_1}, \ldots, x_{i_N}) \Big)^{(-1)^{w(x_1,\ldots,x_m)}} \mod G_{N+1}. \tag{19}$$

If $j \notin \{i_1, \ldots, i_N\}$ then $(\phi_{i_1\cdots i_N}(x_{i_1}, \ldots, x_{i_N}))^c$ will occur in the product above for $(x_1, \ldots, x_{j-1}, 0, x_{j+1}, \ldots, x_m)$ and $(x_1, \ldots, x_{j-1}, 1, x_{j+1}, \ldots, x_m)$, once with exponent $c = 1$ and once with exponent $c = -1$. Accordingly, each term in (19) occurs equally often with exponent 1 as with exponent -1. Since G_N/G_{N+1} is abelian (the corollary to Lemma 3), $u \equiv e \mod G_{N+1}$. Q.E.D.

LEMMA 5. *Fix $N < m$. Assume that $g \in K_m(G_{N+1})$. If*

$$g(x_1, \ldots, x_m) = \prod_{k=N}^{m} \prod_{(i_1,\ldots,i_k)\in I_{m,k}} \phi_{i_1\cdots i_k}(x_{i_1}, \ldots, x_{i_k}) \tag{20}$$

with all $\phi_{i_1\cdots i_k} \in K_k(G_k)$, then there exist $\psi_{i_1\cdots i_j} \in K_j(G_j)$, $(i_1, \ldots, i_j) \in I_{m,j}$, $j = N + 1, \ldots, m$, such that

$$g(x_1, \ldots, x_m) = \prod_{j=N+1}^{m} \prod_{(i_1,\ldots,i_j)\in I_{m,j}} \psi_{i_1\cdots i_j}(x_{i_1}, \ldots, x_{i_j}). \tag{21}$$

Proof. Let $\mu: \{1, 2, \ldots, \binom{m}{N}\} \to I_{m,N}$ be the one-to-one mapping such that if $\mu(i) = (i_1, \ldots, i_N)$ and $\mu(j) = (j_1, \ldots, j_N)$, then $i < j$ if and only if there exists s

such that $i_s < j_s$ and $i_t = j_t$ for $t = s+1, s+2, \ldots, N$. If $\mu(i) = (i_1, \ldots, i_N)$, then $x(\mu(i))$ is defined by

$$x(\mu(i)) = (x_{i_1}, x_{i_2}, \ldots, x_{i_N}). \tag{22}$$

Suppose that

$$g(x_1, \ldots, x_m) = \prod_{i=1}^{N'} \phi_i(x(\mu(i))) \left(\prod_{k=N+1}^{m} \prod_{(i_1,\ldots,i_k)\in I_{m,k}} \phi_{i_1\cdots i_k}(x_{i_1}, \ldots, x_{i_k}) \right), \tag{23}$$

$\phi_i \in K_N(G_N)$, $\phi_{i_1\cdots i_k} \in K_k(G_k)$. By assumption, (23) is valid for $N' = \binom{m}{N}$, and $\mu(1) = (1, 2, \ldots, N)$. If (23) is valid for $N' = 1$, we consider $\phi_1(x_1, \ldots, x_N)$ as a function in $x_1, x_2, \ldots, x_{N+1}$. With this convention $\phi_1 \in K_{N+1}(G_{N+1})$ since g and all $\phi_{i_1\cdots i_k}$, $k > N$, map into G_{N+1}. Using the same rules as in the proof of Theorem 4 when commuting the elements in the product (right-hand side of Eq. (23)), we obtain an expression of the type (21) for g when $N' = 1$.

Suppose then that g has an expression (23) with $N' > 1$. We shall transform it into a similar expression with N' replaced by $N' - 1$. By induction on N' it follows that (20) can be transformed into an expression of the type (21). This is the desired result.

Put $\mu(N') = (j_1, j_2, \ldots, j_N)$. There exist j such that $j < j_N$ and $j \notin \{j_1, j_2, \ldots, j_N\}$ when $N' > 1$. Fix such a j. Let $x_{j_1}, x_{j_2}, \ldots, x_{j_{N-1}} \in X = \{0, 1\}$ be arbitrary. Define $y = (y_1, \ldots, y_m)$, $z = (z_1, \ldots, z_m) \in X^m$ by

$$\begin{aligned} y_{j_N} &= 0, \qquad z_{j_N} = 1, \\ y_i = z_i &= 0 \qquad \text{if} \quad i \notin \{j_1, j_2, \ldots, j_N, j\}, \\ &= x_i \qquad \text{if} \quad i \in \{j_1, j_2, \ldots, j_{N-1}, j\}. \end{aligned}$$

Then

$$\begin{aligned} g(y)\, g^{-1}(z) &\equiv \prod_{i=1}^{N'} \phi_i(y(\mu(i))) \cdot \left[\prod_{i=1}^{N'} \phi_i(z(\mu(i))) \right]^{-1} \\ &\equiv e \bmod G_{N+1}, \end{aligned} \tag{24}$$

since $g(x) \in G_{N+1}$ for all $x \in X^m$. Accordingly,

$$\prod_{i=1}^{N'} \phi_i(y(\mu(i))) \equiv \prod_{i=1}^{N'} \phi_i(z(\mu(i))) \bmod G_{N+1}. \tag{25}$$

Define $a(x_{j_1}, x_{j_2}, \ldots, x_{j_{N-1}}, x_j) \in K_N(G_N)$ and $b(x_{j_1}, x_{j_2}, \ldots, x_{j_N}, x_j) \in K_{N+1}(G_{N+1})$ by

$$a(x_{j_1}, \ldots, x_{j_{N-1}}, x_j) = \prod_{i=1}^{N'} \phi_i(y(\mu(i))), \tag{26}$$

$$a(x_{j_1}, \ldots, x_{j_{N-1}}, x_j)\, b(x_{j_1}, \ldots, x_{j_N}, x_j) = \prod_{i=1}^{N'} \phi_i(x'(\mu(i))), \tag{27}$$

where $x' = (x_1', \ldots, x_m')$ with $x_i' = x_i$ if $i \in \{j_1, j_2, \ldots, j_N, j\}$ and $x_i' = 0$ otherwise.

If $i < N'$ interpret $\phi_i(x'(\mu(i)))$ as a function ϕ_i' in the variable $x(\mu(i))$. Thus (27) is equivalent to

$$\phi_{N'} = \left[\prod_{i=1}^{N'-1} \phi_i'\right]^{-1} a \cdot b. \tag{28}$$

Substitution of (28) in (23) gives

$$g = \prod_{i=1}^{N'-1} \phi_i \left[\prod_{i=1}^{N'-1} \phi_i'\right]^{-1} a \cdot b \left(\prod_{k=N+1}^{m} \prod_{I_{m,k}} \phi_{i_1,\ldots i_k}\right). \tag{29}$$

Using the same rules as in the proof of Theorem 4 when commuting elements in the product (the right-hand side of Eq. (29)), we obtain an expression of the type (23) with N' replaced by $N' - 1$. Q.E.D.

COROLLARY 1. $D(G) = S(G) = \bigcap_{m=1}^{\infty} G_m$.

A subgroup of a decomposable subgroup is always decomposable, while there is no reason that a subgroup of a strongly decomposable group is strongly decomposable. Although the maximum decomposable and strongly decomposable subgroups are equal, the two definitions of decomposability do not lead to identical classes of decomposable groups.

G is self-decomposable if $D(G) = G$. A necessary and sufficient condition for G to be self-decomposable is that $G = G_2$. Since $G_2 = [G, G]$, the commutator subgroup of G, G is self-decomposable if and only if G is its own commutator subgroup. Such groups are called perfect.

COROLLARY 2. *G is self-decomposable if and only if G is perfect.*

COROLLARY 3. *If G is simple and nonabelian, then G is self-decomposable.*

Proof. Since G_2 is normal and $G_2 \neq \{e\}$ when G is nonabelian, $G_2 = G$ in this case. Q.E.D.

A survey of known simple groups can be found in Feit (1970). Among the simple groups are the alternating groups A_n, $n \geqslant 5$, the groups of Lie type, and the Mathieu groups M_{11}, M_{12}, M_{22}, M_{23}, M_{24}. A_n is nonabelian if $n \geqslant 4$. It is well known that any group can be imbedded in an alternating group A_n, and we may choose $n \geqslant 5$. Accordingly; since A_n is decomposable over itself for $n \geqslant 5$:

COROLLARY 4. *Every group can be imbedded in a self-decomposable group.*

Corollaries 3 and 4 can also be found in Kolp (1976). He used quite a different method, depending on the choice of a subgroup of the automorphism group of G.

6. Examples

Let H be a subgroup of G. Suppose the automorphism $\phi: G \to G$ maps H into H. ϕ is called fixpoint free if $\phi(h) = h$ implies $h = e$ when $h \in H$. Elspas and Stone (1967) have given several examples of groups possessing fixpoint free inner automorphisms. Kolp (1972) has shown the following necessary and sufficient condition for H to be imbedded in a group G such that for some $g \in G$, $\phi_g: h \to ghg^{-1}$ is a fixpoint free inner automorphism: H possesses a fixpoint free automorphism.

Elspas and Stone (1967) studied cascades over the binary alphabet $X = \{0, 1\}$, while Kolp (1972) studied cascades over a general alphabet X for groups possessing a fixpoint free inner automorphism. A subgroup H possessing a fixpoint free inner automorphism is decomposable over G as shown by Kolp (1972).

THEOREM 6. *Let H be a subgroup of G possessing a fixpoint free inner automorphism. Then H is strongly decomposable over G.*

Proof. Let $g \in G$ be such that $\phi_g: H \to H$ is fixpoint free. Stone and Elspas (1967) have shown that the mapping $H \to H$ defined by $h \to ghg^{-1}h^{-1}$ is onto in this case. Hence, $H \subset H^*$. By Theorem 1 H is strongly decomposable. Q.E.D.

Let $G = D_n$ denote the dihedral group of order $2n$, generated by the reflections and rotations of a regular polygon with n vertices. If $n = 2^k p$, p odd, then it is easily shown that the maximal m-decomposable subgroup G_m of D_n is generated by $R^{2^{m-1}}$ for $m \geqslant 2$. Here R denotes rotation $2\pi/n$ of the polygon. Accordingly, $D(D_n) \cong Z_p$, isomorphic to the integers modulo p. It is well known (Elspas and Stone, 1967) that Z_p possesses a fixpoint free inner automorphism in D_p and therefore also in D_n. So no new decomposable subgroups of the dihedral group exist even when n is even.

THEOREM 7. *Let $n = 2^k p$, p odd, and put $G = D_n$. If $k = 0$, then $D(G) = G_2 \cong Z_p$. If $k \geqslant 1$, $2 \leqslant m \leqslant k$, then $G_m \cong Z_{p \cdot 2^{k+1-m}}$, while $G_m = D(G) \cong Z_p$ if $m \geqslant k + 1$.*

Let S_n denote the symmetric group of all permutations of n objects, and let A_n be the subgroup of S_n of all even permutations. A_n is called the alternating group.

THEOREM 8. *If $n = 2$ or $n = 3$, then $D(A_n) = G_2 = \{e\}$. If $n = 4$ then $D(A_n) = G_2 = K_4$, the Klein four-group of the double transpositions. If $n \geqslant 5$, then A_n is self-decomposable.*

Proof. A_n is abelian for $n = 2$ or $n = 3$. Hence $G_2 = [G, G] = \{e\}$ in this case. If $n = 4$, then a simple calculation shows that $D(G) = K_4$. If $n \geqslant 5$, then A_n is nonabelian and simple, hence self-decomposable. Q.E.D.

Here the case $n = 4$ is of special interest. Yoeli and Turner (1967) showed that any function f: $X^m \to K_4$ is decomposable over A_4. We have shown that K_4 is the maximal decomposable subgroup of A_4. Also K_4 possesses a fixpoint free inner automorphism in A_4.

THEOREM 9. *If* $n \geqslant 2$, *then* $D(S_n) = [S_n, S_n] = A_n$.

Proof. The case $n = 2$ is trivial. If $n \geqslant 3$ then A_n is generated by the cycles of three elements. Let $h = (a, b, c)$ be an arbitrary three-cycle in A_n. Put $g = (a, b)$, the transposition that commutes a and b. Then $ghg^{-1}h^{-1} = h$. Hence $A_n{}^* \supset A_n$, and A_n is strongly decomposable over S_n. Since $G_2 = [S_n, S_n] = A_n$, $A_n = D(S_n)$. Q.E.D.

Let ϕ: $S_n \to S_n/A_n \cong Z_2$ be the canonical function that maps g into the coset of g mod A_n. From Theorem 9 and Kolp's reduction theorem (Kolp, 1976, Theorem 1) follows the result of Shinahr and Yoeli (1969), that f: $X^m \to S_n$ is decomposable if and only if ϕf: $X^m \to S_n/A_n$ is decomposable. This result can also be found in Klop's paper.

CONCLUDING REMARKS

For certain pairs of groups H, G, $H \subset G$, good cellular cascades have been designed by other authors using the technique of decomposition of group functions. Groups possessing a fixpoint free inner automorphism is such a class. Cellular cascades synthesis based on the results obtained in this paper does not automatically lead to good cascades. Now, however, when the decomposable groups have been characterized, it might be fruitful to look at other groups than those possessing a fixpoint free inner automorphism and investigate if there exist new classes of groups for which cellular cascade synthesis based on decomposition of group functions leads to good cascades.

RECEIVED: November 28, 1975

REFERENCES

ELSPAS, B., AND STONE, H. (1967), "Decomposition of Group Functions and the Synthesis of Multirail Cascades," IEEE Conf. Rec. 8th Ann. Symp. on Switching and Automata theory, pp. 184–196, Austin, Texas.

FEIT, W. (1970), The current situation in the theory of finite simple groups, *in* Actes du Congrès International des Math., pp. 55–93. Nice.

KOLP, O. (1972), The synthesis of multivalued cellular cascades and the decomposition of group functions, *IEEE Trans. Computers* C-21, 489–492.

KOLP, O. (1976), A theory of the cascade decomposition of group functions, *Inform. Contr.* **31**, 216–230.

SHINAHR, I., AND YOELI, M. (1969), Group functions and multivalued cellular cascades, *Inform. Contr.* **15**, 369–376.

YOELI, M., AND TURNER, J. (1967), Decomposition of group functions with applications to two-railed cascades, *Inform. Contr.* **10**, 565–571.

ZASSENHAUS, H. (1956), "The Theory of Groups," Chelsea, New York.